

United States District Court
District of Delaware

REDACTED

In the Matter of the Search of:

PREMISES LOCATED AT

Newark, Delaware

APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT

Misc. No. 05- 82 M

REDACTED

I, Michael S. Armstrong, being duly sworn, depose and say:

I am a(n) Special Agent of the U.S. Secret Service and have reason to believe that

 on the person of or x on the property or premises known as (name, description and/or location)

See Attachment A,

in the District of Delaware

there is now concealed a certain person or property, namely (describe the person or property to be seized)

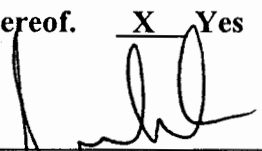
See Attachment B,

which is (state one or more bases for search and seizure set forth under Rule 41(c) of the Federal Rule of Criminal Procedure)
property that constitutes evidence, fruits and instrumentalities of the commission of offenses in violation of Title 18,
United States Code, Sections 471 and 473 (possessing, manufacturing, and dealing in counterfeit currency), among other
offenses.

The facts to support a finding of Probable Cause are as follows:

See attached affidavit of Michael S. Armstrong

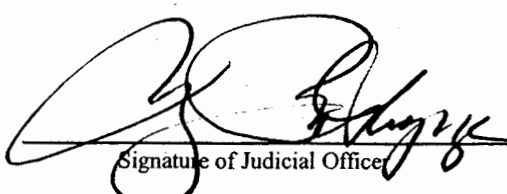
Continued on the attached sheets and made a part hereof. X Yes No


Signature of Affiant
SA Michael S. Armstrong, U.S. Secret Service

Sworn to before me, and subscribed in my presence

May 9, 2005 at Wilmington, Delaware
Date City and State

Honorable Mary Pat Thyng
United States Magistrate Judge
District of Delaware
Name and Title of Judicial Officer


Signature of Judicial Officer

REDACTED

UNITED STATES DISTRICT COURT

DISTRICT OF DELAWARE

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Michael S. Armstrong, being duly sworn, depose and say:

1. I am a Special Agent with the U.S. Secret Service and have been so employed since February 2003. I am currently assigned to the Wilmington, Delaware, Resident Office. My duties include the investigation of counterfeit currency and counterfeit checks. The training given to U.S. Secret Service Special Agents includes approximately six months of field and classroom training in all aspects of the production of genuine United States currency (USC), and the detection of counterfeit currency, including the use of computers in the printing processes, paper production, security features and other identifiers. Prior to my employment with the U.S. Secret Service, I was employed as a Police Officer with the Rehoboth Beach and Bethany Beach Police Departments for five years.
2. I submit this affidavit in support of a search warrant for [REDACTED] Newark, Delaware, as more particularly described in Attachment A. The items to be searched and seized are more particularly described in Attachment B.
3. I am thoroughly familiar with the information contained in this Affidavit based on the investigation that I have conducted in conjunction with the Delaware State Police (DSP). The following information contained in this affidavit is known to me personally or was reported to me by other U.S. Secret Service Agents, DSP officers, and a confidential informant.
4. Because this affidavit is made in support of probable cause to obtain a search warrant, not all of the facts known to me in this investigation are set forth in this affidavit.
5. On March 9, 2005, the DSP arrested an individual on counterfeit charges. He agreed to cooperate with DSP and with Secret Service as a cooperating informant (CI). He said had access to counterfeit U.S. Currency (USC) manufactured by another person.
6. I was introduced to the CI by DSP officers. The CI stated that he has obtained \$12,000.00 in counterfeit USC from Richard Shoemaker of [REDACTED] Newark, Delaware. The CI stated that Shoemaker was manufacturing the counterfeit at his residence in Newark, Delaware. The CI stated that he has also purchased counterfeit checks from him in the past.

7. On March 14, 2005, I obtained a written statement from the CI that he has received \$12,000.00 in counterfeit currency from Shoemaker on two different occasions. In February 2005, he received \$2,000.00 and at the end of February 2005 he purchased another \$10,000.00 in counterfeit from Shoemaker. I obtained Shoemaker's DMV photograph. The CI positively identified Richard Shoemaker of [REDACTED], Newark, Delaware, as the manufacturer of the counterfeit USC. The CI also stated that Shoemaker drives a copper [REDACTED], which was also verified from a Delaware DMV records check. The CI also stated that Shoemaker has [REDACTED] truck.
8. Records from Connective Power show that the customer account at [REDACTED] Newark, Delaware, is in the name of Richard Shoemaker. Connective Power's records show that the account is active, with a last payment date of March 21, 2005.
9. On March 15, 2005, the CI agreed to make a recorded consensual phone call to Shoemaker to order five in counterfeit USC. This phone call was recorded in my presence. During the call, the CI asked for "five", and Shoemaker agreed to meet the CI at Shoemaker's house on March 18, 2005.
10. On March 18, 2005, I drove by Shoemaker's residence at [REDACTED] in Newark. The residence is a white two-story house. There was a [REDACTED] parked in the driveway. Shoemaker has a Jeep registered to him at the above address.
11. On March 18, 2005, the CI came to the Wilmington office of the Secret Service and placed a recorded consensual phone call to Shoemaker. Shoemaker stated that he thought that the CI wanted \$500.00, not \$5,000.00, and he stated he only had \$500.00 but he would try to print the rest by 8:00PM.
12. Later that same day, the CI was fitted with a body wire. Special Agent Al Lassiter and I then searched the CI and his vehicle to ensure that there were no counterfeit funds on his person or in the vehicle. The CI was given \$1,200.00 in government funds to pay Shoemaker for the \$10,000.00 in counterfeit which he had received at the end of February.
13. SA Peter Murphy and I surveilled Shoemaker's residence beginning at 8:05 PM. A white [REDACTED] and a [REDACTED] were parked in the driveway. SA Lassiter followed the CI to Shoemaker's residence, as the CI drove in the same car that was searched for counterfeit. The CI arrived at [REDACTED] in Newark, Delaware, at approximately 8:20 PM. SA Murphy and I observed Shoemaker answer the door and Collier entered the residence, the residence had a porch light. The CI's body wire captured the conversation that ensued between Shoemaker and the CI. Shoemaker stated that, "I'm still printing them", "I have my laptop in the basement running them" and stated "I'll let it run till the ink stops". Shoemaker stated "I have two printers going, fronts on one and

backs on the other". Shoemaker stated "I'll go out in the morning to get ink and I'll run them all day tomorrow". Shoemaker discussed that the backs of the bills were a little off.

14. Shoemaker only gave the CI \$1,660.00 in counterfeit USC. At approximately 8:25 PM, SA Murphy, and I observed the CI exit the residence and get into his vehicle. SA Lassiter followed the vehicle back to our meeting location. The CI went to our meeting location and handed me what he thought was approximately \$2,000.00 in counterfeit USC. The CI stated that Shoemaker was making the rest of the money. The CI stated that he saw Shoemaker cut one sheet of counterfeit on a paper using a cutter located in his dining room area. The \$20.00 counterfeit Federal Reserve Notes ("FRNs"), serial number CF54038187D is the same number that was recovered from the CI when he was arrested at the Concord Mall.
15. On April 27, 2005, the CI agreed to make a recorded consensual phone call to Shoemaker to order \$15,000.00 in counterfeit USC. This phone call was recorded in my presence and Shoemaker stated, "I have nine printed up". Shoemaker then stated, "my intentions were to keep printing a bunch of it up, so I had it." Shoemaker stated that its' all good, unlike the \$5,000.00 I was trying to get together and its all good I threw out all the garbage, its nice". Shoemaker then stated, "it will take me no time to print up the rest." Shoemaker asked the CI if he was going to cut it. Shoemaker then stated, "if you want to hook up tomorrow night I can give you what I have". Shoemaker finished by saying that he has already recouped the money he has spent on ink.
16. On May 3, 2005, the CI contacted me and stated that Shoemaker had contacted him and said he had \$9,000.00 in counterfeit with him and he wanted to meet the CI to give him the money.
17. On May 3, 2005, at approximately 1:30 PM, the CI agreed to make a recorded consensual phone call to Shoemaker to arrange for the delivery of the counterfeit. The CI asked Shoemaker if he has been to his house to pick up the counterfeit. Shoemaker stated, "No, Tracey (Shoemaker's wife) was there, we could hook up first thing in the morning." Shoemaker told the CI that he would call him in about an hour to arrange for the delivery.
18. Later on May 3, 2005, the CI agreed to make a recorded consensual phone call to Shoemaker to arrange for the delivery location. Shoemaker told the CI to meet him at the Shell Station on Delaware Avenue in Wilmington, DE at 3:30 PM. Shoemaker stated, "I have to go home to gather up everything."
19. Later that same day, the CI was fitted with a body wire. Special Agent Peter Murphy and I then searched the CI and his vehicle to ensure that there were no counterfeit funds on his person or in the vehicle. SA Andrew Balceniuk and CPL. Anthony Easterling, Wilmington Police Department, went to the Shell Gas Station

on Delaware Avenue to set up for surveillance. Upon their arrival, they contacted me and told me that Shoemaker was already there in his w [REDACTED] truck. Upon the CI's arrival, at approximately 3:47 PM, SA Balceniuk observed Shoemaker hand the CI a small cardboard box and watched them talk for a few moments and the CI leave.

20. SA Peter Murphy and I followed the CI to the gas station and set up surveillance across the street. SA Murphy monitored the body wire. The conversation between the CI and the target was recorded and the following statements were obtained from the recording. The CI asked about the quality of the counterfeit, Shoemaker stated, "some of them are off" and, "it looks good, it's a pain in the ass, I have to go to the basement behind my heater". The CI asked Shoemaker about the printing process, and Shoemaker stated, "if this keeps up I am going to invest in a color laser printer and I have to find a program." The CI told Shoemaker he may need more counterfeit, Shoemaker replied, "I'm going to keep printing them".
21. The CI was observed leaving the gas station at approximately 3:50 PM. The surveillance on the CI was broken for approximately seven minutes, due to Cpl. Easterling receiving a domestic assault in progress call near the Shell station. Once at our office, SA Balceniuk recovered the small brown box which contained counterfeit \$20.00 FRNs. The counterfeit recovered was the same serial number as the counterfeit FRNs, which were recovered in the previous transaction from Shoemaker at his residence. I searched the CI's vehicle and no other contraband was located. The small cardboard box contained \$15,820.00 in counterfeit \$20.00 FRNs, all with the serial number CF54038187D.
22. Based on my experience and training regarding the practices of persons involved in computer crimes, the manufacturing of checks and/or CFT currency it is customary for them to possess and utilize a personal computer and associated communications and peripheral equipment, including modems, scanners, CI readers/writers, backup tape drives, printers, and floppy discs.
23. Based on my experience and training regarding the production of counterfeit USC. The criminals use a scanner and printer to manufacture counterfeit USC. The process consists of placing genuine currency onto the scanner, scan the image and print the front of the USC. Then you flip the USC and copy the back. The fronts are put back into the printer and the backs are printed. The process is time consuming due to the fact that the placement of the currency on the scanner glass has to be exact so the fronts and backs line up. The possession of the laptop computer, scanner, and printer, from my experience is a mobile counterfeit USC plant.
24. Based on my experience and training, I am aware that many "high tech" criminals tend to be proud of their work and they tend to retain much of their work, even if stored in encrypted or hidden formats on their computer systems. Further, even

computer files that have been intentionally deleted can still be recovered, wholly or in part, through forensic analysis by an expert. Further, some computer

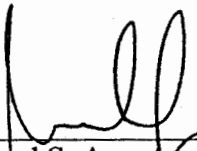
25. Based upon my experience and knowledge, I know that searches and seizures of evidence from computers commonly requires agents to seize most or all computer items (hardware, software, and instructions or manuals) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:
26. Computer storage devices (such as hard disks, diskettes, tapes, laser disks, Bernoulli drives, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site; and
27. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search, which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even "hidden", erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.
28. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices, as well as the central processing unit (CPU). In addition the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

///

29. Based on my investigation, there is probable cause to believe that Richard Shoemaker is making counterfeit money in his residence. There is also probable cause to believe that Shoemaker is using a lap top computer and all its associated parts and peripherals as an instrumentality of manufacturing counterfeit checks and counterfeit USC. These acts are known me as being in violation of Title 18, United States Code Section 471 and 473, as well as 18 USC 1030 (a)(5)(A)(Fraud and related Activity in Connection with Computers).

WHEREFORE, your affiant prays that this Court issue a warrant for the search of Shoemaker's residence, as more particularly described in Attachment A, for the seizure of the items described with more particularity in Attachment B.

Your affiant, having signed this Affidavit under oath as to all assertions and allegations contained herein, states that its contents are true and correct to the best of his knowledge, information and belief.



Michael S. Armstrong
Special Agent
United States Secret Service

SUBSCRIBED AND SWORN TO
BEFORE ME THIS 9 DAY
OF May, 2005.



THE HONORABLE MARY PAT THYNGE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF RESIDENCE TO BE SEARCHED

██████████ Newark, Delaware 19711. The residence is a two story home, with white siding, green shutters and front door, a front facing garage, it is located in the middle of the block, and it backs up to railroad tracks. The residence is located in the ██████████ community.

ATTACHMENT B

LIST OF ITEMS TO BE SEARCHED FOR AND SEIZED OR COPIED

1. Computers containing data related to the manufacturing of counterfeit currency and checks.
2. Electronically stored data, files or digital information relating to the manufacturing and passing of counterfeit currency and counterfeit checks, stored on the computers hard drive(s), software, or associated media to include diskettes, tapes, CD Roms, DVD's, Zip Disks, Jazz Disks or any peripheral storage devices to include PDA devices, external/internal storage devices and Cameras
3. Deleted, altered, damaged or corrupted data stored in the same areas related to counterfeit currency or counterfeit checks.
4. Computer System information and file structure data necessary to access the data in items 2 and 3.
5. Recovered Software to include system operations software and device management software that is necessary to access and understand the data in items 2 and 3.
6. Electronically stored information verifying ownership of the aforementioned computer system and associated software including registration information.
7. Any records, notes, Passwords or personal identification numbers (PINS), names, addresses, telephone numbers, correspondence, emails and chat logs relating to the manufacturing or passing of counterfeit currency and counterfeit checks
8. Any counterfeit currency and counterfeit checks in the residence.
9. Any receipts for the purchase of ink, paper and/or any contraband for the manufacturing of counterfeit currency and/or counterfeit checks.
10. Any and all computers, printers and scanners in the residence.

This warrant is for the seizure of the above described computer data and for authorization to read, retrieve, copy and seize information stored and contained on the above describes data sources and for authorization to present these items to persons capable of conducting such examinations and recovery.

The search procedure for electronic data contained in computer operating software or memory devices, whether performed on site or in a laboratory, or other controlled environment, may include the following techniques:

1. Surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files.

